量子情報通信理論の基礎と最近の話題 : エントロピー, エンタングルメント, アルゴリズム, テレポーテーション (符号と暗号の代数的数理)

AUTHOR(S):

大矢, 雅則

CITATION:

大矢, 雅則. 量子情報通信理論の基礎と最近の話題 : エントロピー, エンタングルメント, アルゴリズム, テレポーテーション (符号と暗号の代数的数理). 数理解析研究所講究録 2005, 1420: 68-82

ISSUE DATE:

2005-04

URL:

http://hdl.handle.net/2433/47182

数理解析研究所講究録 1420 巻 2005 年 68-82

量子情報通信理論の基礎と最近の話題 ～エントロピー，エンタングルメント，アルゴリズム，テレポーテーション～

大矢　雅則
東京理科大学　理工学部　情報科学科
千葉県野田市山崎 2641

1　はじめに

量子情報理論は，確率論を基にしたシャノン流の古典的な情報通信理論では扱えない量子的な対象－例えば，光の量子状態やさらに一般的な量子エンタングルド状態（二つ以上の系の干渉性を包含した状態）－を用いた情報の表現と通信を，量子確率論や量子エントロピー論をベースにして取り扱う理論である．それゆえ，量子情報の研究は，古典情報理論の非可換（量子）版として数理物理的色彩の強いものであった．現在，この量子情報の研究は，２１世紀のＩＴ，例えば，圧倒的な計算速度を持つ量子コンピュータ，究極的な通信と考えられている量子テレポーテーション，盗聴に対する安全性が非常に高いと思われる量子暗号などと深くかかわって来ている．

2　情報と通信

この節では，情報通信の数理表現のエッセンスを説明する．A を入力情報を記述するアルファベットの集合（もっと一般的な集合でもよい）とする:$A=\{a_1,a_2,\cdots,a_n\}$. このとき入力空間 Ω は，A の無限直積

$$\Omega=A^Z\left(\equiv\cdots\times A\times A\times\cdots=\prod_{-\infty}^{+\infty}A\right)$$

で与えられる．この入力空間が通信路にとって都合がよいものであれば Ω で記述された情報をそのまま通信路へ送ればよいが，そうでないときは，Ω と通信路に

とって都合のよい他の空間 X との対応を考える必要がある．そこで「Ω から X への可測写像 ξ を符号化とよぶ」

一般に上の写像 ξ には1対1であることを要求する場合が多いがここでも特に断わらない限りこれを仮定する．

さて，あるメッセージ ω_k の生起確率を p_k とし，こうしたメッセージの列を伝送するとする．このとき，この列 $\{\omega_k\}$ の有する情報量（エントロピー）は生起確率 $p=\{p_k\}$ の関数として

$$S(p)=-\sum_k p_k \log p_k$$

で与えられる．この確率分布 p はメッセージの状態を表していると言われる．それゆえ，メッセージ自体やメッセージの列を入力状態と呼ぶことになる．これらの入力状態を物理的に設計された通信路に送るとき，メッセージそれ自体やメッセージの列の情報量がどれほど正しく送られたかが問題になる．そうした議論のために次に必要になるのは通信路の数理である．

入力状態を記述する空間を上記のように $(\Omega,\mathfrak{F}_\Omega)$ とし（ただし，$\mathfrak{F}_\Omega$ は σ 集合体），符号化された入力状態を記述する空間を X とする．この X は生の入力空間同様，可測空間の場合もあり，ヒルベルト空間などの場合もある．通常（古典系）の情報理論では可測空間となる．入力空間同様，出力空間も符号化されたままの空間 X' と情報源と同様なアルファベットから作られる空間 Ω'（多くの場合 $\Omega'=\Omega$）上で記述される．チャネルとは X から X' への写像のことである．この写像を λ で表すと，入力状態 ω がある仕方 ξ で符号化され，それがチャネル λ を通して伝送され，それが復号化 $\overline{\xi}$ によって元のアルファベット（$\Omega=\Omega'$ の場合を考えて）にもどされるプロセスは次のようにかける．

$$\omega \to \xi(\omega)\lambda \longrightarrow \lambda\circ\xi(\omega) \to \overline{\xi}(\lambda\circ\xi(\omega)) \tag{1}$$

このとき $\overline{\xi}(\lambda\circ\xi(\omega))\neq\omega$ となる確率を入力情報 ω に関する誤り確率という．なお，$\Omega'\neq\Omega$ の場合には，ω に対応する ω' が何らかの仕方で分かっていなければならないが，このときは，$\overline{\xi}(\lambda\circ\xi(\omega))\neq\omega'$ となる確率が誤り確率である．それ故，$\Omega=\Omega'$ の場合，通報される M 個の情報を $\omega^{(1)},\cdots,\omega^{(M)}$ とし，それらの先験的な生起確率を $p\left(\omega^{(k)}\right)$ とすると，誤り確率は

$$P_e=\sum_{k=1}^{M} p\left(\omega^{(k)}\right) p\left(\overline{\xi}\left(\lambda\circ\xi\left(\omega^{(k)}\right)\right)\neq\omega^{(k)}\,\middle|\,\omega^{(k)}\right)$$

で与えられることになる．そこで，この誤り確率を最小にする符号化 ξ，チャネル λ，復号化 $\overline{\xi}$ を見いだすことが問題となるのである．

この通信過程の基本は，ω の生起確率と，ω を符号化した $\xi(\omega)$ の生起確率は同じであるから，空間 X の状態（これも以下入力状態と呼ぶ）から空間 X' の状態（出力状態）への変換ということになる．この入力状態を出力状態に移す写像をチャネルという．したがって，チャネルとは（1）の X 上の確率分布の集合，確率測度の集合，密度行列の集合などのいわゆる状態の集合から X' 上の状態の集合への写像ということになる．この写像を以下 Λ^* で表す．"$*$"がつく意味は後で解るであろう．また，記号上の便宜さから出力空間を，以下では，X' ではなく，Y で表すことにする．

ここで，古典離散系のチャネルと相互エントロピー（情報量），そのチャネルの効率を評価する通信路容量について説明しておこう．

古典系では入力空間と出力空間は共に可換な確率空間によって記述される．特に，離散系では，この状態は確率分布で表せることになる．入力系 X の状態 $p=\{p_i\}_{i=1}^n$ から出力系 Y の状態 $q=\{q_i\}_{i=1}^m$ への離散系のチャネル Λ^* とは，

$$\Delta_n=\left\{p=\{p_i\}_{i=1}^n, \sum_{i=1}^n p_i=1, p_i\geq 0\,(i=1,\cdots,n)\right\}$$

から Δ_m への写像である．例えば，2つの完全事象系 X,Y とそれぞれの系の分布 p,q を

$$X=\begin{pmatrix} x_1,\cdots,x_n \\ p_1,\cdots,p_n \end{pmatrix}, p=\begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix}, \quad Y=\begin{pmatrix} y_1,\cdots,y_n \\ q_1,\cdots,q_n \end{pmatrix}, q=\begin{pmatrix} q_1 \\ \vdots \\ 1_n \end{pmatrix}$$

で与えると，系 X から系 Y への次の遷移確率行列 Λ^*(すなわち，$q=\Lambda^* p$)

$$\Lambda^*=\begin{pmatrix} p(y_1|x_1) & p(y_1|x_2) & \cdots & p(y_1|x_n) \\ \vdots & \vdots & \ddots & \vdots \\ p(y_m|x_1) & p(y_m|x_2) & \cdots & p(y_m|x_n) \end{pmatrix} \tag{2}$$

はチャネル である．

さて，シャノンの大きな発見ともいえる相互エントロピーを説明しよう．いま，2 で与えられるチャネルを通じて入力状態 p が伝送されたとき，出力状態 q は，

$$q=\Lambda^* p=(q_j)=\left(\sum_{k=1}^n p(y_j|x_k)\,p_k\right)$$

で与えられ，複合事象系 $X \times Y$ 上の確率分布（同時分布）は

$$r = \{r_{ij} = p(x_i, y_j)\} = \{p(y_j|x_i)\, p_i\}$$

となる．ここで，

$$p \otimes q \equiv (p_i q_j) = \left(p_i \sum_{k=1}^{n} p(y_j|x_k)\, p_k \right)$$

とおくと，入力系 X の分布 $p = \{p_i\}_{i=1}^{n}$ と出力系 Y で得られる分布 $q = \Lambda^* p$ に関する相互エントロピーは，p とチャネル Λ^* で決まり，相対エントロピーを用いて次のように定められる．

$$I(p; \Lambda^*) = S(r, p \otimes q) := \left(\sum_{j=1}^{m} \sum_{i=1}^{n} r_{ij} \log \frac{r_{ij}}{p_i q_j} \right)$$

なお，この離散系の相互エントロピーを下にして，連続系の相互エントロピーはコロムゴロフやヤグロムによって定式化されている．

相互エントロピーとエントロピーは次の基本不等式を満たす（シャノンの基本不等式）：

$$0 \leq I(p; \Lambda^*) \leq \min\{S(\rho), S(\Lambda^* p)\}$$

それ故，相互エントロピーとエントロピーの比

$$e(\Lambda^*) = \frac{I(p; \Lambda^*)}{S(p)}$$

がチャネル Λ^* の効率を測る尺度の一つになる．

この節の最後にチャネル効率を測る基本量である通信路容量について記しておこう．符号化 ξ，チャネル λ，復号化 $\bar{\xi}$ の共役写像をそれぞれ $\Xi^*, \Lambda^*, \bar{\Xi}^*$ で表すと，1 の通信過程は

$$p \to \Xi^*(p) \to \Lambda^* \circ \Xi^*(p) \to \bar{\Xi}^* \circ \Lambda^* \circ \Xi^*(p) = \bar{p}$$

で表せることになる．今，入力系の確率分布（状態）の全体 $P(\Omega)$ の部分集合 S を実際に使用可能な状態の集合とするとき，この集合に関する通信路容量は

$$C^S\left(\bar{\Xi}^* \circ \Lambda^* \circ \Xi^*\right) \equiv \sup\left\{I\left(p; \bar{\Xi}^* \circ \Lambda^* \circ \Xi^*\right); p \in S\right\}$$

で定められ，これを最大にする $\Xi^*, \Lambda^*, \bar{\Xi}^*$ を決めることが通信理論の問題となる．

3 量子系の情報量と通信過程

さて，話を量子系に移そう．量子系の入力・出力空間は，一般的には，C^* 代数を使って記述されるが，ここでは簡単のため，ヒルベルト空間上で話を進める．

光ファイバを使って通信を行う現代の情報伝送では，情報は量子系の状態を用いて表さなければならない．すなわち，情報を量子状態によって符号化する必要がある．今，シンボル $a_k \in A$ に対応する（表す）量子状態を ρ_k とする．さらに，簡単のため，アルファベット空間Aあるいはその第一段の符号化空間 X を2つの元からなる空間 $\{0,1\}$ とする．

$$A = \{0,1\} \Leftrightarrow \Xi = \{\rho_0, \rho_1\}$$

この空間 Ξ の例の一つとして，ρ_0 を真空状態，ρ_1 をコヒーレント状態やスクイーズド状態等で表される．この符号化の詳細は省略せざるを得ないが，今，情報をある量子状態 ρ(例えば，上記の ρ_0, ρ_1 の凸結合）を表せたとし，これを光ファイバのような適当な物理的媒体を用いて伝達するとする．媒体と外界からの雑音等の影響が，状態を変化させ，それが受信側へ伝達されるのである．したがって，チャネルとは入力状態への媒体と外界からの影響を表すものであり，数学的には状態の変化を与える写像である．$\mathcal{H}_1, \mathcal{H}_2$ をそれぞれ入力側，出力側のヒルベルト空間とし，$B(\mathcal{H}_k)$ を $\mathcal{H}_k$ 上の有界線形作用素の全体，$\mathfrak{S}(\mathcal{H}_k)$ を $\mathcal{H}_k$ 上の密度作用素（量子状態）の全体とする．そこで，$\mathfrak{S}(\mathcal{H}_1)$ から $\mathfrak{S}(\mathcal{H}_2)$ への写像 Λ^* を量子力学的チャネルといい，アファイン性 (すなわち，$\sum_n \lambda_n = 1$ ならば $\Lambda^*\left(\sum_n \lambda_n \rho_n\right) = \sum_n \lambda_n \Lambda^*(\rho_n), \rho_n \in S(h_1)$) を満たす Λ^* を線形な量子力学的チャネルという．さらに，$B(\mathcal{H}_2)$ から $B(\mathcal{H}_1)$ への Λ^* の共役写像 Λ とは，任意の $\rho \in S(h_1)$ と任意の $A \in B(h_2)$ に対して，$tr\Lambda^*(\rho) A = tr\rho\Lambda(A)$ が成り立つものをいうが，この Λ が完全正写像であるとき，Λ^* を完全正な量子力学的チャンネルと呼ぶ．なお，Λ が完全正写像であるとは，任意の $n \in N$ と任意の $A_j \in B(h_2)$ と任意の $B_k \in B(h_1)$ に対して，$\sum_{j,k=1}^{n} B_j^* \Lambda\left(A_j^* A_k\right) B_k \geq 0$ を満たす場合をいう．詳しい説明は省略するが，様々な物理系におけるほとんどすべての状態の変換は，このチャネルの特殊な場合なのである．

量子系におけるチャネルの定義を与えたが，ここで，この一例として，光通信過程を念頭において，通信過程に侵入してくる雑音と漏れ出ていく損失を陽に考慮した，チャネルの数学的構成法を説明しておく．

今，入力系と出力系のヒルベルト 空間 $\mathcal{H}_1$ と $\mathcal{H}_2$ に加えて，外部効果を記述する二つのヒルベルト空間 $\mathcal{K}_1, \mathcal{K}_2$ を用意する．ここで，$\mathcal{K}_1$ は雑音系のヒルベルト空間とし，$\mathcal{K}_2$ は損失系のそれとする．

さて，3つの写像 a^*, π^*, γ^* を次のように定める：

(1)a^* は $\mathfrak{S}(\mathcal{H}_2 \otimes \mathcal{K}_2)$ から $\mathfrak{S}(\mathcal{H}_2)$ への写像であり

$$a^*(\theta) = tr_{k_2}\theta, \theta \in \mathfrak{S}(\mathcal{H}_2 \otimes \mathcal{K}_2)$$

で与えられる.

(2) π^* は $\mathfrak{S}(\mathcal{H}_1 \otimes \mathcal{K}_1)$ から $\mathfrak{S}(\mathcal{H}_2 \otimes \mathcal{K}_2)$ への写像であり，これは媒体それ自体の物理的特性から決まるものである．減衰過程や増幅過程はこの写像によって特徴付けられている.

(3) γ^* は $\mathfrak{S}(\mathcal{H}_1)$ から $\mathfrak{S}(\mathcal{H}_1 \otimes \mathcal{K}_1)$ への写像であり，雑音を表す状態を σ とすると，

$$\gamma^*(\rho) = \rho \otimes \sigma$$

で与えられる.

こうして，光通信における量子力学的チャンネル Λ^* は

$$\Lambda^*(\rho) = a^* \circ \pi^* \circ \gamma^*(\rho) = tr_{k_2}\pi^*(\rho \otimes \sigma), \rho \in \mathfrak{S}(\mathcal{H}_1)$$

と書き表される．従って，雑音 σ と合成系間のチャンネル π^* がわかれば，光通信系のチャンネル Λ^* が構成できたことになる．この構成法に従い，σ と π^* を適当に与えてやると量子通信路を通して情報を伝送したときの伝送容量，誤り確率などを導くことができるのである.

シンボル $\{0,1\}$ を符号化した量子純粋状態 $\left\{\rho_0^{(1)}, \rho_1^{(1)}\right\}$ がチャネル Λ^* を通じて出力側へ送られたとする．このとき，チャネルがZ型，すなわち，シグナル"0"は常に "0"に送られ，"1" は誤って "0"に送られるときと，"1"などの"0"以外の状態に送られる（このとき，"0"以外の状態を"1"と見なし，正しく送られたとする）ことがあるとする．このとき，"1 → 0"の誤り確率 P_e は

$$\begin{aligned} P_e &= tr\Lambda^*\left(\rho_1^{(1)}\right)\rho_0^{(2)} \\ &= tr_{\mathcal{H}_1}\left(tr_{\mathcal{K}_1}\pi^*\left(\rho_1^{(1)} \otimes \sigma\right)\right)\rho_0^{(2)} \end{aligned}$$

で与えられるのである,

次に，量子系における状態の有する情報量の表現であるエントロピーについて論じよう．量子系のエントロピーの定式化は1930年頃フォン・ノイマンによって，密度作用素 ρ で表される状態に対して

$$S(\rho) = -tr\rho\log\rho$$

と定められた．ところで，状態 $\rho \in \mathfrak{S}(\mathcal{H})$ のスペクトルは離散的であるから，そのスペクトル分解は，一意に，

$$\rho = \sum_n \lambda_n P_n$$

と書ける．ここで λ_n は ρ の固有値，P_n は $\mathcal{H}$ から λ_n に関する固有空間への射影作用素である．従って，各 λ_n に縮退がなければ，P_n の値域の次元は 1 である（これを，$\dim P_n = 1$ と書く）．ある固有値 λ_n が縮退している場合は，$\dim P_n \geq 2$ であるが，この P_n は 1 次元射影作用素に更に分解される：

$$P_n = \sum_{j=1}^{\dim P_n} E_j^{(n)}$$

ここで，$E_j^{(n)}$ は 1 次元作用素で，ρ の λ_n に関する固有ベクトルを $x_j^{(n)}$ $(j = 1, \cdots, \dim P_n)$ とすると $E_j^{(n)} = \left|x_j^{(n)}\right\rangle \left\langle x_j^{(n)}\right|$ である．これらの 1 次元射影 $\left\{E_j^{(n)}\right\}$ の添字 j, n を適当に付け変えて，

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq \cdots, \quad E_n \perp E_m$$

とすると，スペクトル分解は

$$\rho = \sum_n \lambda_n E_n$$

と書ける．この分解をシャッテン分解とよぶことにする．なお，上式において，重複度が 2 以上の固有値はその回数だけ繰り返し現われている．たとえば，λ_1 の重複度が 2 のときは，$\lambda_1 = \lambda_2$ である．また，単純でない固有値に対する射影 P の分解は一意でないことから，すべての固有値が単純でなければ，シャッテン分解も一意ではない．以下，とくに断らない限り，ρ と σ は $\mathfrak{S}(\mathcal{H})$ の元とし，$\rho = \sum_n \lambda_n E_n$ と書けば，これはシャッテン分解とする．このシャッテン分解を用いると量子系のエントロピーは，確率分布 $\{\lambda_k\}$ のシャノンのエントロピーになる．つまり，

$$S(\rho) = -\sum_k \lambda_k \log \lambda_k$$

となる．このエントロピー $S(\rho)$ は古典系のエントロピーと単調性をのぞいてほぼ同様な性質を有している．量子系の相互エントロピーは，古典系の同時確率分布に代わるものとして導入された量子力学的合成状態を用いて大矢によって定式

化されたが，これを説明する前に，古典系のカルバックとライブラーの相対エントロピーの量子版について話す必要がある．2つの状態 $\rho,\sigma\in\mathfrak{S}(\mathcal{H})$ に関する量子系の相対エントロピーは，梅垣によって，

$$S(\rho,\sigma)\equiv\begin{cases} tr\rho(\log\rho-\log\sigma) & (s(\rho)\leq s(\sigma)) \\ +\infty & \text{その他}\end{cases}$$

と定められた．ここで，$s(\rho)$ は ρ の台（$tr\rho(I-E)=0$ となる最小の射影作用素 E）である．

いま，入力状態 $\rho=\sum_k\lambda_kE_k$ に対して，初期状態 ρ と終状態 $\Lambda^*\rho$ の間に存在する相関を示す合成状態 σ_E は $\mathcal{H}_1\otimes\mathcal{H}_2$ 上に

$$\sigma_E=\sum_n\lambda_nE_n\otimes\Lambda^*E_n$$

と定められる．ここで，この分解は $E=\{E_n\}$ の選び方に依存するので添え字 E を付してある．この合成状態は古典系の同時確率分布（または，同時確率測度）に対応するもので，初期（入力）状態と終（出力）状態の相関を表すものである．これを用いると，初期状態 ρ がチャネル Λ^* によって $\Lambda^*\rho$ に変換されたとき，ρ の有する情報のどれほどが終状態 $\Lambda^*\rho$ に伝えられたかを表す量である相互エントロピーは，

$$I(\rho;\Lambda^*)=\sup_E S(\sigma_E|\sigma_0)=\sup_E\left\{\sum_k\lambda_kS(\Lambda^*E_k|\Lambda^*\rho)\right\}$$

で定められる．ここで，σ_0 は，$\sigma_0=\rho\otimes\Lambda^*\rho$ で与えられる自明な合成状態である．この相互エントロピーは次の基本的不等式を満たす．

なお，この相互エントロピーは初期状態 ρ が古典的なものであれば，ρ のシャッテン分解が一意になり，E_n はデルタ測度 δ_n になる。このとき，$I(\rho;\Lambda^*)=\sum_k\lambda_kS(\Lambda^*\delta_k|\Lambda^*\rho)$ と書ける。さらに，この特殊な場合がHolevoやLebitinによって論じられた，古典一量子系の相互エントロピーである。相互エントロピーは基本不等式

$$0\leq I(\rho;\Lambda^*)\leq\min\{S(\rho),S(\Lambda^*\rho)\}$$

を満たす。

この $I(\rho;\Lambda^*)$ を使って量子通信における様々な尺度が定められるのである．例えば，与えられたチャネル Λ^* とある適当な量子状態の集合 S に対して送信できる情報量の最大値である純量子通信路容量は次のように与えられるのである：

$$C^s(\Lambda^*)=\{I(\rho;\Lambda^*);\rho\in S\}$$

なお，ここで論じた密度作用素に対するエントロピーと相互エントロピーは，通常の測度論的定式化をその特殊な場合として含む，より一般的な C^*-力学系においても定式化されている．例えば，相対エントロピーは荒木によって一般のフォンノイマン代数上の状態のそれに拡張され，ウールマンは更に$*$-代数上の正の線形汎函数に関するそれに拡張した．また，相互エントロピーも一般の C^* 代数上で大矢によって論じられている．さらに，この相互エントロピーを用いて，量子系の一般化された力学（ＫＳ）エントロピーを定式化することや力学系のカオスを分類することなどができるのである．

4　量子コンピュータ

最近，膨大なデータを高速に演算処理する新しい計算機システムの構築がさまざまな形で試みられている．その最有力候補として実現が期待されているのが，原子や分子それ自体が作るエンタングルド状態（後述）を利用して高速で演算を行う量子コンピュータである．量子コンピュータが高速計算を可能にする主な理由は，量子力学に従う論理ゲートが計算ステップを（原理的に）大幅に減少させる点にあるが，これは量子状態の干渉性に大きく依存している．すなわち，量子コンピュータは量子状態の強い干渉性を利用して，いくつかの独立な計算を一度に行うことを可能にするのである．

各升目に０か１の書かれたテープをヘッドが読み，書き換えていく古典コンピュータ（チューリング機械）において，基本的なのは０か１の書かれた各升目であった．「０か１」のかわりに，０か１かそれらの重ね合わせか，を考えるのが量子コンピュータである．すなわち，計算といえば，今までは古典系の古典論に従うものを考えていたのだが，量子系で量子力学に従う計算を考えようというのが量子コンピュータである．量子コンピュータの実現は，現在まだ，難しいが，理論的には非常に興味深い結果が得られている．

量子コンピュータの動作を０か１だけに（重ね合わせを許さず）制限すれば，これは古典コンピュータとなる．すなわち，量子コンピュータは古典コンピュータを含むものである．では，重ね合わせを許すメリットは何か．その一つの例としてショアーのアルゴリズムがある．ショアーは古典コンピュータでは非常に時間がかかり現実的には不可能であった因数分解が，量子コンピュータでは現実的な時間 (入力サイズに対して多項式時間）で解けることを示した．これが実現されれば，因数分解を鍵として用いている今現在の暗号技術は大きな変革を迫られることになる．

何故量子コンピュータが速い計算を可能にするのか．第一の理由は重ね合わせ状態の干渉性に起因する計算の従属性（並列性）にある．古典コンピュータにおいては，解の候補が，例えば，１万個あれば，最悪，一つ一つ確かめて１万回の計算を行わなければならなかった．ところが，量子コンピュータの場合，計算の

入力として，その１万個の重ね合わせ状態というものをとることができる．すると，計算自体は一回（程度）ですみ，その結果，解を含む重ね合わせが得られることになる．量子コンピュータで，大切なことは，その重ね合わせからうまく解を取り出すことになる．また，そこが非常に難しいことでもある．すなわち，解を含む重ね合わせ状態（１万個のベクトル状態の）が得られても，単に観測を行えば，解が得られる確率は，最悪の場合は，１万分の１で，結局，古典コンピュータと同様，１万回の試行が必要になってしまう．ショアーのアルゴリズムは，解でない部分の位相がうち消し合い，その部分の和が０になるため，残された重ね合わせの個数が非常に少なくなり，かなりの確率で解を取り出せるという方法であった．

量子計算を数理的に記述すると以下のようになる．

(1) まず，入力，計算，出力全てを記述する複素ヒルベルト空間 $\mathcal{H}$ を用意し，この中から入力状態ベクトルを決める．それを

$$\psi = \sum_k c_k \psi_k$$

とする．ここで，$\{\psi_k\}$ はヒルベルト空間 $\mathcal{H}$ の基底であり，c_k は $\sum_k |c_k|^2 = 1$ を満たす複素数である．

(2)ψ を適当なユニタリー・ゲート (プログラムに従って作られる) により変換して $\bar{\psi}$ を得る．

$$\bar{\psi} = \sum_k \bar{c}_k \psi_k$$

(3)$\bar{\psi}$ を観測して，観測結果から望ましいものを選ぶ．このために，他の方法 (古典計算機などを用いて) による判定を用いても良い．通常量子計算は，０，１の重ね合わせである量子ビットを用いるので，今のところヒルベルト空間 $\mathcal{H}$ としていくつかの２次元複素ヒルベルト空間 $\mathbb{C}^2$ のテンソル積ヒルベルト空間 $\otimes_1^n \mathbb{C}^2$ を考えることが多い．

ショアーの研究の後をうけて，筆者とロシアのヴォロビッチは，1999 年～2002 年，「NP 完全問題が P 問題になるアルゴリズムが存在するか?」という 30 年来の問題を研究した．我々は，量子アルゴリズムにカオス力学の非線形な状態変化のアイデアを導入することによって，NP 完全問題の一つである SAT（Satisfiability；充足可能性）の問題を多項式時間で解くアルゴリズムを見いだした．これは，量子コンピュータとカオスシステムを組み合わせたカオス量子コンピュータとも呼びうる新しいシステムの提案である．詳しいことは割愛せざるを得ないが，以下 NP 完全問題とは何か，SAT とは何か，を説明し，我々の方法の骨子を記しておこう．

入力のサイズが n の問題に対して，P 問題，NP 問題，NP 完全問題とは次のように定められている．

P 問題 ： サイズ n の入力に対して，ある問題（計算）をあるアルゴリズムに従って解く（行う）とき，計算機がその問題（計算）を解き終わる（終了する）までの時間が入力サイズ n の多項式で表せる時間ですむとき，そのアルゴリズムは良いアルゴリズムであるといい，その問題はクラス P（polynomial）に属する問題という．

NP 問題：問題の解の候補を具体的に与えたとき，これが本当に解になっているかを検算することはサイズ n の多項式時間でできるが，解自体を求めることは多項式時間でできるかどうか分かっていない問題のことをいう．$(P \subset NP)$

NP 完全問題：NP に属する問題のうち最も難しいと考えられている問題が NP 完全問題と言われ，しかも全ての NP 完全問題はどれも同じ難しさであることが分かっている．

この NP 完全問題の一つが **SAT 問題**で，それは，「与えられたブール代数式（"変数，カッコ，AND（∧）,OR（∨）,NOT（¬）"から構成される論理式）を"1（真）"とする（充足する）変数に真偽を与える仕方（関数）t は存在するか？」という問題である．もう少し数学的に表すと次のようになる，ある要素の集合 $\{x_1, \cdot\cdot, x_n\}$ とその部分集合 $X_j \subset \{x_1, \cdot\cdot, x_n\}$ に対して，$X\prime_j \subset \{\neg x_1, \cdot\cdot, \neg x_n\}, C_j \subset X_j \cup X\prime_j, C = \{C_1, \cdots, C_m\}$ と置き，各要素に 0 または 1 を対応づける真偽値関数 t とし，$f(\mathbf{x}) \equiv \wedge_{j=1}^{m}(\vee_{x \in C_j} t(x))$ をブール式と呼ぶ．このとき，SAT 問題は「$f(\mathbf{x}) = 1$ を満たすような真偽値関数 t が存在するか？」という問題になる．

この SAT 問題は量子アルゴリズムとカオス増幅計算により多項式時間で解けることが分かる．そのアウトラインを以下説明しよう．

入力ベクトル $\mathbf{x} = \{x_1, \ldots, x_n\}$，ブール式 $f(\mathbf{x}) \equiv \wedge_{j=1}^{m}(\vee_{x \in C_j} x)$ に対して，SAT 特有の計算を行うユニタリー作用素を U_f とする（これは具体的に構成できる）．まず，離散フーリエ変換によって初期状態 $|\mathbf{x}, 0\rangle$ は重ね合わせ

$$|v\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} |\mathbf{x}, 0\rangle$$

に変換される．次いで，U_f を用いて，$f(\mathbf{x})$ を計算すると，$|v\rangle$ は

$$|v_f\rangle = U_f |v\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} |\mathbf{x}, f(\mathbf{x})\rangle$$

となる．最後の qu ビットを測定し，$f(\mathbf{x}) = 1$ を得る確率を調べると，それは $r/2^n$ となる．ここで，r は $f(\mathbf{x}) = 1$ の解の個数である．つまり，終状態ベクトルは

$$|v_f\rangle = \sqrt{1 - q^2}\, |\varphi_0\rangle \otimes |0\rangle + q\, |\varphi_1\rangle \otimes |1\rangle$$

で表せる．ここで，$|\varphi_1\rangle$ と $|\varphi_0\rangle$ は正規化された n 量子ビットの状態で，$q = \sqrt{r/2^n}$.

以上で SAT 問題の量子計算は終わる．r が測定できるほど十分大きな値であれば，SAT 問題は解けたことになるが，r が小さければ，解が存在するかどうかわからない（測定できない）．そこで，r が小さい場合も考慮して，q を観測せず，それを増幅することを考えなければならない．このために必要なのがカオス増幅である．つまり，量子アルゴリズムと非線形な（カオティックな）状態変化を組み合わせれば，NP 完全問題が多項式時間で解けることになる．

我々の方法はカオスを起こす非線形写像を用いていることから，通常の量子アルゴリズムのみ，すなわち，ユニタリー変換のみで処理し仕切れるものではなく，ユニタリー計算を越えた計算が必要になる．さらに，上記の議論は，今の所，純粋に数学的アルゴリズムに過ぎず，今後このアルゴリズムを実現する物理過程とは何かを明らかにすることも必要であろう．なお，このアルゴリズムは最近一般化された Turing 機械によって記述できることが示されている。

5 量子テレポーテーション

最後に，究極的な量子通信とも言える量子テレポーテーションについて説明しよう．量子状態に情報を乗せそれをある通信路を用いて伝送し，量子状態そのものを受け手に送ることができるとすれば，量子状態の堅牢性（すなわち，観測をすると量子状態は多くの場合壊れてしまうこと）より，気付かれず盗聴をすることが非常に難しいことになる．そこで，

「いかなる通信路を用いれば，量子状態それ自体の伝送が可能か？」

が問題となる．このことは素朴なプロトコル（古典，量子問わず従来の通信路）では不可能である．究極の通信プロトコルといえる量子テレポーテーションでは次に説明する量子エンタングルド状態を用いて量子状態それ自体の伝送を可能にするのである．量子エンタングルド状態とは，二つの量子系 A と B において，例えば，「A が 0 で B が 0」な状態と「A が 1 で B が 1」な状態の重ね合わせ状態 $\psi := \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$ などをエンタングルド状態（絡み合った状態）と呼び，系 A と系 B はエンタングルしているという．この例では，系 A が 0 であるか 1 であるかを測定してみると，これは確率半々で得られるが，系 A が 0 である時には，系 B で"0 か 1 か"を測定しても常に 0 であることになる．こうしたエンタングルド状態を用いることによって新たな通信が可能になるのである。

量子テレポーテーションはアリスが任意の量子状態を，そのままの形で，ボブに伝送する過程である．これができれば，あらゆる情報は量子状態で表せるので，完璧な情報伝送が可能になるし，アリスが量子コンピュータで行っていた計算経過をその途中でボブにバトンタッチするようなことも可能になる．

アリスが送りたい任意の状態を記述する系を系 1 と呼ぶ．まず，アリスが系 1 の状態そのものを，それが記述している内容を知ることなしに，ボブに安全に

伝えるということはできるだろうか．そのために，以下のような装置とプロセスを考えればよい．アリスは系１の他に系２も持ち，ボブは系３を持っていて，それらはある量子状態を介してエンタングルしている．

系１と系２が結合して作られている，目盛を持った測定器に，アリスは送りたい状態を入れ（観測をし）て，その後，その状態をボブに送る．すると，系２と系３の間のエンタングルド性によって，系３（ボブ）の状態が作られる．

アリスは先ほどの測定器の目盛りを読んで，その目盛りを電話等，古典的な手段でボブに伝える（ブロードキャスト）．例えば，「ランプは”３”がついているわ.」などとアリスがボブに伝えることになる．最後に，その測定結果を聞いたボブは，対応した操作を系３に移った状態にほどこす．

以上の操作が量子テレポーテーション過程の操作である．ところで今，ここに第三者イブがいたとして，いったいイブは何をできるだろうか．イブが出来ることは，せいぜいアリスがブロードキャストした測定結果を傍受することぐらいである．ところが，これを知っても，イブにはアリスとエンタングルした系はもともとないのだから，何もすることはできない．このようにこれは安全な通信過程でもあることがわかる．

このテレポーテーション過程は，最初，ベネット等によってＥＰＲ状態を用いて定式化された．この方法は数学的には簡単なものであるが，実現には様々な問題があった．そこで，大矢とフィットナーは，１９９９～２００２年，コヒーレント状態をもちいた量子テレポーテーションを提案し，定式化した．

5.1 量子テレポーテーションの数理

以下，量子テレポーテーションの数理を説明しよう．アリスの持つ２つの系はヒルベルト空間 $\mathcal{H}_1, \mathcal{H}_2$ で記述されるとし，系１の送りたい未知の状態を ρ とする．また，ボブはヒルベルト空間 $\mathcal{H}_3$ を持つとする．量子テレポーテーション過程は以下の４つのステップに分けることができる．

Step1:アリスのもつ系２とボブのもつ系３はエンタングルさせる．つまり，エンタングルド状態 $\sigma \in \mathfrak{S}(\mathcal{H}_2 \otimes \mathcal{H}_3)$ を準備する．

Step2:アリスは，与えられた ρ と σ の合成状態 $\rho \otimes \sigma \equiv \rho^{(123)}$ （$\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3$ 上の状態）において，$\mathcal{H}_1 \otimes \mathcal{H}_2$ 上の適当な射影作用素 $(F_{nm})_{n,m=1}^{N}$ によって作られた物理量 $F \equiv \sum_{n,m=1}^{N} z_{nm} F_{nm}$ を一回測定する．アリスは F の固有値の一つ「z_{nm}」を測定結果として得る．測定後の全系 $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3$ の状態は $\rho_{nm}^{(123)} \equiv$

$(F_{nm}\otimes)\,\rho\otimes\sigma\,(F_{nm}\otimes)$ になる．ボブは，状態

$$\Lambda^{*}_{nm}(\rho) = tr_{12}\rho^{(123)}_{nm}$$
$$= tr_{12}\frac{(F_{nm}\otimes \mathbf{1})\,\rho\otimes\sigma\,(F_{nm}\otimes \mathbf{1})}{tr_{123}\,(F_{nm}\otimes \mathbf{1})\,\rho\otimes\sigma\,(F_{nm}\otimes \mathbf{1})}$$

を得る．

Step3:アリスは測定結果「z_{nm}」をボブに普通の仕方で伝える．例えば，電話で「z_{nm}」を得たことを伝える．

Step4:ボブは聞いた結果「z_{nm}」に対応する"ＫＥＹ"を系３に施す．この"ＫＥＹ"はユニタリー作用素の組$\{W_{nm}\}$で，前もってボブに与えられている．「z_{nm}」に対応する"ＫＥＹ W_{nm}"をステップ２で得られた状態に施すと，ボブの状態は

$$W_{nm}\Lambda^{*}_{nm}(\rho)W^{*}_{nm} = [(F_{nm}\otimes W_{nm})(\rho\otimes\sigma)(F_{nm}\otimes W^{*}_{nm})]$$

になる．これが，状態ρに一致すれば，テレポーテーションが成功したことになる．したがって，量子テレポーテーションの問題は，"エンタングルド状態$\sigma\in\mathfrak{S}(\mathcal{H}_2\otimes\mathcal{H}_3)$，物理量

$$F\equiv\sum_{n,m\,=\,1}^{N} z_{nm}F_{nm}$$

及び，"ＫＥＹ"$\{W_{nm}\}$が存在して，

$$W_{nm}\Lambda^{*}_{nm}(\rho)W^{*}_{nm} = \rho$$

となるか"を問う問題になる．

量子テレポーテーションには，一回の伝送で，ρを完全に送るもの（完全量子テレポーテーション；ＣＱＴと略記）と，数回の伝送でρを完全に送るもの（不完全量子テレポーテーション；ＩＣＱＴと略記）とに分けられる．情報伝送に限れば，２回，３回，アリスがρを送っても構わないので，実質的な差はない．

なお，完全な量子テレポーテーションのためには完全にエンタングルした状態（すなわち，等確率振幅で重ね合わされた状態）が必要であることと，このエンタングルド状態を長時間作ることはけして簡単な事ではないので，ＣＱＴよりＩＣＱＴの方が実現性が高いことは断るまでもない．

ベネット等による EPR ペアーを用いたプロトコルは完全量子テレポーテーションの一例であり，大矢・フィットナーのフォック空間上のコヒーレント状態を用いたプロトコルは完全量子テレポーテーションと不完全量子テレポーテーション両方の例を与えている．

なお，本解説の詳細，特に情報理論，量子情報に関しては [1]，量子エントロピーの数理は [2]，量子アルゴリズム，コンピュータ，暗号，テレポーテーションの研究レベルの解説は [3] 量子暗号，テレポーテーションは [4] に説明している。

References

[1] R.S. Ingarden, A. Kossakowski and M. Ohya,"Information Dynamics and Open Systems", Kluwer, 1997.

[2] M. Ohya and D. Petz: "Quantum Entropy and its Use", Springer-Verlag, 1993.

[3] M.Ohya and I.V.Volovich, "Mathematical Foundation of Quantum Information and Computation", Springer—Verlag to be published.

[4] 大矢，渡辺，宮寺；"新たな量子通信ー量子暗号と量子テレポーテーションー" 共立出版，近刊